Claims:

What is claimed is:

Claim 1. A method for defeating, in a server unit of an IP (Internet Protocol) network, a SYN flooding attack, said server unit running TCP (Transport Control Protocol) to allow the establishment of one or more TCP connections with one or more client units, said method comprising the steps of:

upon having activated TCP in said server unit:

listening for the receipt of a SYN message sent from one said client unit;

upon receiving said SYN message:

computing an ISR (Initial Sequence number Receiver side);

responding to said client unit with a SYN-ACK message including said computed said ISR:

resuming to said listening step.

Claim 2. The method according to claim 1 wherein the step of computing said ISR further includes the steps of:

concatenating a randomly generated key with an identification of one said TCP connection said identification including:

a client socket and a server socket;

hashing said concatenation, thus obtaining a server signature;

concatenating said server signature and a category index referring to a set of predefined TCP connection categories;

thereby, obtaining a computed ISR.

Claim 3. The method according to claim 1 or 2 wherein said computing step further comprises the steps of:

updating, in said server unit, a pseudo-random number (PRN) generator;

holding a current key;

remembering a former key; and

using said current key as said randomly generated key for said computed ISR.

Claim 4. The method according to claim 2 wherein the step of concatenating said category index includes the further step of:

picking up a category index within said set of predefined connection categories on the basis of the content of said received SYN message.

Claim 5. The method according to claim 3 wherein said updating step includes the step of:

updating said PRN generator at a rate not higher than an MSL (Maximum Segment Lifetime) defined in said TCP connection.

Claim 6. A method for defeating, in a client unit of an IP network, a SYN flooding attack, said method comprising the steps of:

upon receiving a SYN-ACK message from a server unit:

normally responding with an ACK message, said step of normally responding comprising the step of:

including, in said ACK message, a computed ISR incremented by one.

Claim 7. A method for defeating, in a server unit of an IP network having a TCP connection, a SYN flooding attack, said method comprising the steps of:

upon having activated TCP in said server unit:

listening for the receiving of an ACK message sent from one client unit;

upon receiving said ACK message:

checking an ISR;

if failing said checking step:

dropping said ACK message;

if passing said checking step:

decoding said ISR as being an authentic computed ISR;

allocating resources for said TCP connection according to content of said computed ISR;

establishing said TCP connection;

in either case:

resuming said listening step.

Claim 8. The method of claim 7 wherein the decoding step includes the step of :

interpreting a category index extracted [[688]] from said computed ISR.

Claim 9. The method according to claim 8 wherein the allocating step includes the step of:

selecting a predefined set of parameters, for said TCP connection, on the basis of the value of said category index.

Claim 10. The method according to claim 7 wherein the step of checking said ISR includes, upon receiving said ACK message, the steps of:

having, firstly, selected said current key:

getting said selected key;

concatenating said selected key with an identification of said TCP connection, said identification including:

a client socket and a server socket;

hashing said concatenation, thus obtaining a re-computed server signature;

extracting an acknowledgment field from said ACK message;

decrementing content of said acknowledgement field;

extracting said server signature;

comparing said re-computed server signature and said extracted server signature;

if said extracted server signature and said re-computed server signature match:

extracting said category index; if said extracted server signature and said re-computed server signature to not match:

checking if a second loop status is set;

If not set:

selecting a former key [[698]];

setting a second loop status;

resuming execution at said getting step;

if set:

failing said checking step.

Claim 11. A computer program product for defeating, in a server unit of an IP (Internet Protocol) network , a SYN flooding attack, said server unit running TCP (Transport Control Protocol) to allow the establishment of one or more TCP connections with one or more client units, said computer program product having computer readable program code comprising the steps of:

upon having activated TCP in said server unit:

computer readable program code for listening for the receipt of a SYN message sent from one said client unit;

upon receiving said SYN message:

computer readable program code for computing an ISR (Initial Sequence number Receiver side) ;

computer readable program code for responding to said client unit with a SYN-ACK message including said computed said ISR:

computer readable program code for resuming said listening step.

Claim 12. The computer program product according to claim 11 wherein the step of computing said ISR further includes the steps of:

computer readable program code for concatenating a randomly generated key with an identification of one said TCP connection said identification including:

a client socket and a server socket;

computer readable program code for hashing said concatenation, thus obtaining a server signature;

computer readable program code for concatenating said server signature and a category index referring to a set of predefined TCP connection categories ;

thereby, obtaining a computed ISR .

Claim 13. The computer program product according to claim 11 or 12 wherein said computing step further comprises the steps of:

computer readable program code means for updating, in said server unit, a pseudo-random number (PRN) generator;

computer readable program code for holding a current key;

computer readable program code for remembering a former key; and

computer readable program code for using said current key as said randomly generated key for said computed ISR.

Claim 14. A system for implementing a shield for defeating TCP SYN flooding attacks said system comprising:

an IP (Internet Protocol) network;

a server unit running TCP (Transportation Control Protocol) to allow the establishment of one or more TCP connections; and

one or more client units; wherein, once said TCP is activated in said server unit, said server unit listens for the receipt of a SYN message from one or more of said client units; and whereupon receiving said SYN message, said server unit computes an ISR (Initial Sequence number Receiver side), responds to said client unit with a SYN-ACK message including said computed ISR and resumes listening for further SYN messages.